AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jeremy Thompson, a Task Force Officer with the United States Secret Service (USSS) being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, LLC (Google), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a duly sworn police officer with the City of South Charleston, WV since May 2011, and have been assigned as a Task Force Officer with the United States Secret Service (USSS) in Charleston, WV since December 2017. My investigative duties focus primarily on conducting criminal investigations involving forgery, bank fraud, false loan applications, wire fraud, credit card fraud, false identification, financial elder abuse investigations, money laundering investigations, identity theft and other financial crime investigations.

3. I received 16 weeks of training at the West Virginia State Police Academy, which centered on criminal investigations including financial crimes. As a task force officer with the USSS, I have been involved in numerous financial elder abuse/romance frauds investigations. I know from my training and experience that those persons involved in committing those types of crimes spend a great deal of time each week seeking out potential victims through email, text messages, social media websites such as Google Hangouts, Go Fish, Plenty of Fish and various dating sites. I also know that people who commit these crimes stay in constant contact with victims, creating a friendship that ultimately leads to a false romantic relationship with victims. I know that these fraudsters tell their victims untrue stories about their employment, their personal life, their family life and their need for financial assistance. In many of these instances, the fraudsters propose marriage to the victim. I know that after this romance flourishes, the fraudsters then ask victims to send them money for various reasons. Some of the fraudsters' reasons include family medical emergencies, or because the fraudsters need to pay their oilrig workers, or need money to ship gold or other valuables back to the United States to be allegedly shared with the victims or finally, for bail when the fraudsters were allegedly arrested after leaving a foreign country.

4. I know from my training and experience that these fraudsters instruct their victims to send large amounts of currency through the U.S. Mail, FedEx and through the United Parcel Service (UPS). I know that these fraudsters get their victims to send money to them via cashier checks, personal checks, money orders, wire transfers, bitcoin and through many different mobile payment processing companies. These mobile payment processing companies include

Transferwise, Ping Express, Money Gram, Western Union, Walmart, Boss Revolution, Pay Pal, Square, Cash App, Xoom, Zelle, and others.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents/officers and witnesses.

6. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit is taken from financial records, interviews with witnesses, and information shared with me from other investigators and state officials. This ongoing investigation is financial in nature, thus, any figures I cite in this affidavit are based on calculations and tracing conducted to date and may be subject to revision at a later date.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code (U.S.C.) §§ 371, 1341, 1343, 1344, 1349,1956-1957, as well as 31 U.S.C. § 5324 have been committed by Kenneth Chukunomnazu EMENI ("EMENI"), John Rabesh NASSY ("NASSY"), Abdul Illal OSUMANU ("OSUMANU"), Augustine C Chukwu Noe AMECHI, also known as Augustine A Chukwu Noe ("AMECHI"), Kenneth Oseme OGUDU also known as Kenneth Lee ("OGUDU"), Oluwagbenga Temitope HARRISON ("HARRISON"), Kayode Gbolahan AKANBI ("AKANBI"), Abiodun Oluwatosin AFOLABI also known as Benik Afobe ("AFOLABI"), and Oluwabanishe Taofik AWOLESI ("AWOLESI"). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

TARGET EMAIL ADDRESSES

9. This affidavit is seeking search warrants for the following email addresses, (collectively, these email addresses are referred to as the "Target Email Addresses"):

markwilliams3672@gmail.com;

bindaryautotrade65@gmail.com;

smithinayee@gmail.com;

01robbenjack@gmail.com;

jackwils1598@gmail.com;

richardclem121@gmail.com;

i.amida101@gmail.com;

billblanco1965@gmail.com;

teddydrey90@gmail.com;

johncolns286@gmail.com;

ginar4940@gmail.com;

jj1082427@gmail.com;

emenikenneth5@gmail.com;

rabeshn@yahoo.com;

nassy@marshall.edu;

illalcapito28@yahoo.com

achukwu45@yahoo.com

b.mastermind2016@gmail.com

kennethogudu52@gmail.com

martinun242@gmail.com

harrisonoluwagbenga@gmail.com

tosiopz@yahoo.com

baawelosi@gmail.com

10. The following target email addresses were used by fraudsters when communicating with the victims and are discussed in the Victim Information section of the affidavit (collectively, the email addresses will be referred to as the "Victim Contact Email Addresses"): markwilliams3672@gmail.com; bindaryautotrade65@gmail.com; smithinayee@gmail.com; 01robbenjack@gmail.com; jackwils1598@gmail.com; richardclem121@gmail.com; i.amida101@gmail.com; billblanco1965@gmail.com; teddydrey90@gmail.com; johncolns286@gmail.com; ginar4940@gmail.com; jj1082427@gmail.com

11. The investigation has revealed that the following email addresses are associated with EMENI , NASSY, OSUMANU , AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI. The Financial Analysis Section of this affidavit will discuss how EMENI , NASSY, OSUMANU , AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI used the following email addresses when opening accounts with various financial institutions and mobile payment processing companies (collectively, these email addresses will be referred to as the "Subjects Financial Contact Email Addresses"). The investigation also revealed that in 2019, World Remit emailed AMECHI, OGUDU, and AFOLABI, to provide financial documentation or an explanation for several of the suspicious transactions that occurred from their World Remit accounts. OGUDU responded to World Remit's email requesting more information about his transactions from an email address, which appears to be registered to a Martin Graham, even though he signed the email as Kenneth OGUDU. OGUDU claimed that funds in his account came from his income as a cars salesman. However, this claim is inconsistent with both OGUDU's known wage information and the types of financial transactions that appear in his accounts.

Similarly, the investigators also learned that on May 1, 2019, AMECHI wrote to Remitly that the company had blocked him from sending money to his family and friends

a. EMENI's known email address is emenikenneth5@gmail.com. This email address in connection with his profiles and financial transactions on multiple mobile payment processing websites, including Zelle, Xoom, Remitly, Transfer Wise, and World Remit.

b. NASSY's known email addresses are rabeshn@yahoo.com and nassy@marshall.edu. Per subscriber data learned from Oath Holdings, rabeshn@yahoo.com is registered to a NASSY Rabesh and the backup email is nassy@marshall.edu. Nassy@marshall.edu is the email address Marshall University provided NASSY. These email addresses are connected to NASSY's profile and financial transactions conducted through mobile payment processing websites and financial institutions. Both email addresses, rabeshn@yahoo.com and nassy@marshall.edu are associated with his Zelle profile. The nassy@marshall.edu address is associated with his City National Bank and World Remit accounts.

c. OSUMANU's known email address is illalcapito28@yahoo.com. Per Oath Holdings this email is registered to OSUMANU. He has used this email address in connection with his profile and financial transactions on multiple mobile payment processing websites, including Zelle, Xoom, and Venmo.

d. AMECHI's known email address is b.mastermind2016@gmail.com, mastermind2016@gmail.com, and achukwu45@yahoo.com. Per Oath Holdings, achukwu45@yahoo.com is registered to Augustine Chuku. He has used this email address in connection with his profile and financial transactions on multiple mobile payment processing websites, including Zelle, Chase Bank, TransferWise. Augustine for Remitly and transfers for Xoom, Venmo, WorldRemit. The b.mastermind2016@gmail.com is connected to AMECHI's World Remit, Remitley and Zelle transactions and accounts. The mastermind2016@gmail.com is connected to AMECHI's Xoom transactions.

e. OGUDU's known email address is kennethogudu52@gmail.com and martinun242@gmail.com. These email addresses were used in connection with his profile and financial transactions on multiple mobile payment websites. OGUDU used the email address kennethogudu52@gmail.com in connection with his Transfer Wise transactions, and Fifth Third bank accounts. He used the email address martinun242@gmail.com in connection with his World Remit transactions.

f. HARRISON's known email addresses are harrisonoluwagbenga@gmail.com and oluwagbenga.harrison@yahoo.com. His google email address was used in connection with his profile and financial transactions on multiple mobile payment websites, Stripe and World Remit, whereas he used the yahoo email addressed in connection with Remitly.

g. AFOLABI's known email address is tosiopz@yahoo.com. Per subscriber data learned from Oath Holdings, tosiopz@yahoo.com is registered to a Tosin AFOLABI. This email address was used in connection with his profile and financial transactions on a mobile payment website, World Remit.

h. AWOLESI's known email address is baawolesi@gmail.com. This email address was used in connection with Chase Bank account.

BACKGROUND

12. EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI are a group of individuals who have lived in the Huntington, WV and most of these persons attended Marshall University in Huntington, WV. All of these persons listed above, with the exception of AWOLESI, are citizens of Nigeria and/or Ghana. AWOLESI is a United States citizen. AMECHI is now a dual citizen of the United States and Nigeria. EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI appear to be part of an organization who have been involved in orchestrating international mail/wire/bank fraud scams wherein members of the organizations have collected over three million dollars from victims located throughout the United States and abroad.

13. Scammers – who may be EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and ANWOLESI or their known and unknown co-conspirators - have contacted potential victims all over the world, using alias' initially striking up friendships with the victims. The scammers contacts would occur frequently and the scammers

would eventually tell the elderly victims they were in love with them and would propose marriage. Many victims fell in love with the scammers and would accept these proposals.

14. Many times the scammers would communicate with their victims by text, Google Hangouts, Instagram, Go Fish and other websites. The scammers also contacted the victims by cell phone and via email. Yet, the scammers would refuse to FaceTime with the victims, in an effort to conceal their true identities. In most instances, scammers would communicate with their victims for several weeks before the scammer would ask their victims for financial help. The scammers would provide false information to their victims including false names, false occupations, false locations where they allegedly resided and worked, false information about their need for financial assistance, and false information about their family situation.

15. The investigation has uncovered numerous victims who have funneled large amounts of money to EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and ANWOLESI at the direction of various online scammers. EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and ANWOLESI have also transferred a large amount of money between themselves during the fraud. Their criminal activity dates back to at least 2017 and has continued until at least the spring of 2020. EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and ANWOLESI are being investigated for violations of 18 U.S.C. §§ 1341, 1343, 1344 (mail, wire, and bank fraud respectively) and 1956, 1957 (money laundering) as well as violations of 31 U.S.C. § 5324, among other statutes.

VICTIM[1] INFORMATION

16. Investigators interviewed multiple individuals, who they currently believe to be victims who transferred money to EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI's bank accounts. Information that investigators learned from the victims and financial records are described below. One similarity uniting all of the victims is that they transferred the money to EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI upon the requests of the online fraudsters, even though the victims themselves did not know or ever communicate with men they knew to be EMENI, NASSY, OSUMANU, AMECHI, OGUDU, HARRISON, AKANBI, AFOLABI, and AWOLESI.

Victim 1

17. In late 2017 or early 2018, Victim 1 met a man on Facebook who went by the name of Robben Jack ("Robben"). They communicated via email or text messages almost every day, sometimes multiple times a day. Robben communicated to Victim 1 with the email address 01robbenjack@gmail.com. Robben sent Victim 1 what he claimed were videos and photographs of himself. Robben told Victim 1 he was from Nigeria, and was currently working as an engineer on an oilrig located off the coast of the United Kingdom. Robben also told Victim 1 that he did not have access to his bank accounts in Nigeria. The company he allegedly worked for was located

[1] Investigators currently believe that the individuals labeled Victim 1 through Victim 25 are fraud victims. However, investigators may change their classification of these individuals if they learn more information which shows that one of the victims is more appropriate classified as a co-conspirator or a money mule.

in Dubai. After they had been communicating for a while, Robben told Victim 1 he was coming to the United States on vacation and they would get married. Robben's company allegedly told Robben he would have to find a replacement for him while he was on vacation and Robben would have to pay the replacement for the period he would be gone from the oilrig.

18. Robben told Victim 1 he could not pay his replacement because he could not access his bank accounts, and if he could not pay for his replacement he could not travel to the United States and marry her. Robben asked Victim 1 to wire Kenneth EMENI the money and EMENI would forward the money to him. Victim 1 wired $5,750 from her Pennsylvanian account to EMENI's bank account held in West Virginia on or about February 28, 2018.

19. Victim 1 stated she sent Robben several I Tune cards 2-3 times before she sent the wire transfer to EMENI. She believes she sent the iTune cards to EMENI at Jack's direction. Robben kept emailing her until December 2018 asking for money, but she refused to send additional funds.

Victim 2

20. On September 14, 2019, Victim 2 was on a social media site, when she met a man who told her his name was Martin Aldrin ("Martin"). Martin told Victim 2 he was from Nixa, Missouri. Martin also claimed he was a civil engineer, and an independent contractor who was working on an oilrig in Alaska. Victim 2 communicated with Martin frequently, through texting and Google Hangouts. Martin changed his phone numbers frequently.

21. Shortly after they started communicating, Martin asked Victim 2 for money because he had a difficult time paying his personal and business expenses while working in Alaska

on the oilrig. Initially, Victim 2 purchased gift cards from Amazon, Ebay and Google. Victim 2 would take a photo of the back of the gift cards and then send Martin the photos through Google Hangouts or via text messages.

22. On November 4, 2019, Martin asked Victim 2 to send a $5,000 wire transfer to Kenneth EMENI in Huntington, WV, via City National Bank in Charleston, WV. Martin told Victim 2 the purpose of this wire transfer was to purchase supplies for the oilrig. Victim 2 didn't know EMENI, but sent the wire as Martin requested and the payment reference on the wire transfer form was "Supplies/Aldrin."

23. Victim 2 stated that this romance fraud ended in December 2019 when Martin advised Victim 2 that his real name was not Martin and he was actually a 19 year old from Lagos, Nigeria. The 19 year old would not disclose his actual name but he did tell Victim 2 that he was tired of lying to her. The 19 year old told Victim 2 he was working with his older brother on this romance fraud. He further told Victim 2 that his role in the fraud scheme was to contact Victims and lie to them to get money and his older brother's role in the scheme was to handle the money generated by the fraud. The 19 year old told Victim 2 he was ending the romance fraud with her because his older brother was reading all of the messages between him and Victim 2.

Victim 3

24. Victim 3, who resides in Massachusetts, first met a man online who told her his name was John Bogus ("John"). They communicated through Google Hangouts. John asked Victim 3 for money and Victim 3 sent this man money through Kenneth EMENI on multiple occasions. Victim 3 stated John Bogus gave her instructions to send the money to Kenneth

EMENI. On October 26, 2017, she sent $2,500 through Western Union to EMENI, on November 9, 2017, she sent $1,300.00 through Western Union to EMENI; and finally, on December 13, 2017, she sent $500.00 through Western Union to EMENI. Victim 3 stated the romance scam ended when she couldn't afford to send any additional money to John Bogus.

Victim 4

25. In early 2019, Victim 4 met a man online who went by the name of Richard Clem ("Richard"). They communicated almost every day and sometimes several times a day via text messages, email and by phone. Richard's email was richardclem121@gmail.com. Richard told Victim 4 he was from Beverly Hills, CA. Richard also told Victim 4 that he had bank accounts at City Bank in California. Richard told Victim 4 he was a Lieutenant in the U.S. Army and the Army sent him to Scotland on a peacekeeping mission. Richard repeatedly requested that Victim 4 send him money for a variety of reasons. For example, Richard told Victim 4 he had one son, who was injured in a car accident and that he needed money to pay the son's hospital bills. Richard also told Victim 4 that while in Scotland, he and his platoon discovered a gold mine and all members of the platoon bought into the gold mine. Richard asked Victim 4 for money to pay workers who mined the gold for him and for funds to ship some of the gold back to the United States. Richard told Victim 4 that he (Richard) was involved in a car accident himself and he was the only survivor. Richard told Victim 4 due to the car accident he had accumulated doctor's bills and he needed surgery to save his leg. Victim 4 sent funds to Richard via at least 15 different individuals. On March 2, 2020, Victim 4 wired $3,000, from her bank account in Las Vegas, Nevada to AMECHI's bank account held in Huntington, West Virginia, per Richard's instructions.

Victim 5

26. Victim 5 advised investigators that he met a woman he knew as Amida Ibrahim ("Amida") online around the middle of 2017. Amida used the email address i.amida101@gmail.com. She advised Victim 5 she was born in Canada and moved to Ghana to attend a culinary school. Amida told Victim 5 she was in her mid-30s. Victim 5 advised they communicated almost every day, usually on Google Hangouts and other sites. It was about 8-10 months after they met online before Amida asked Victim 5 for any money. Victim 5 recalled the first time Amida asked for money was supposedly to pay for dormitory expenses at her school. At Amida's suggestion, Victim 5 went to an Indiana Walmart and sent her approximately $200.

27. Approximately 3-4 weeks after Victim 5 sent the initial $200, Amida frequently asked Victim 5 for more money to pay for living expenses. Victim 5 would then either send money through Walmart or purchase iTunes cards that he sent to Amida. Victim 5 recalled one occasion when Amida asked Victim 5 to send her a new iPhone because hers was not working. Victim 5 refused to send her an iPhone. However, during one of their conversations, Amida told Victim 5 that he would be receiving a package from a friend of hers and the package would contain a new iPhone. Amida told Victim 5 the package would be pre-addressed and she wanted Victim 5 to forward the package to a friend of hers, Abdul Illah OSUMANU and that OSUMANU would forward the package to her in Ghana. Following Amida's request, Victim 5 sent the iPhone to OSUMANU in Huntington, WV.

28. During the summer of 2018, Amida told Victim 5 that she had recently inherited about $7,500,000 in gold bars after her father's death. She further told Victim 5 that for her to

collect the gold bars she had to pay approximately $750,000 in inheritance taxes to Ghana and that she could not afford the taxes. Amida asked Victim 5 for help paying the taxes. Amida told Victim 5 that a friend of hers and her fathers, Dr. Eric Gborn, was also going to provide funds to pay these taxes. Amida gave Victim 5 Dr. Gborn's email address, billblanco1965@gmail.com. Victim 5 stated he emailed Dr. Gborn several times. Victim 5 wrote personal checks in 2018 and 2019 to help Amida pay the inheritance taxes. Per Amida's instructions, Victim 5 made the checks payable to OSUMANU. After Victim 5 sent the checks, Amida informed him that she received the money.

29. The checks Victim 5 sent Amida through OSUMANU are shown by the chart:

Date	Check Number	Amount
9/5/2018	3011	$3,000
9/21/2018	3014	$500
10/19/2018	3016	$10,000
11/19/2018	3017	$5,700

30. Around March 18, 2020, Victim 5 wrote a check for $6,500 which was made payable to Faridu Iddrisu, per Amida's instructions. Amida told Victim 5 to make the check payable to Faridu Iddrisu because he is a friend of hers and Iddrisu would forward the money to her. Amida told Victim 5 she had received the $6,500 shortly thereafter.

Victim 6

31. Around February 2018, Victim 6, who resides in New Hampshire, met a man on Facebook who stated his name was David Gedrile ("David"). She eventually switched her

communications with David to Facebook Messenger, and then she switched to Google Hangouts. David told Victim 6 that he lived in Texas and that he worked on an oilrig in the Caribbean. Victim 6's romance with David lasted from February 2018 to the fall/winter of 2018. According to Victim 6, she and David talked daily during this time.

32. Early in the romance, David told Victim 6 he needed some money as a loan. David told Victim 6 that he had bank accounts in the United Kingdom, which he could not access because he was working on an oilrig in the Caribbean. Victim 6 sent money to David on several occasions. David would instruct her to send the funds to various individuals and David told her that these individuals would forward the funds to him. Victim 6 sent money or items to the individuals listed below at the direction of David:

(a) On April 2, 2018, Victim 6 sent David $1,500.00 for permission to travel to the Caribbean because David did not have access to his accounts in the United Kingdom. Victim 6 was supposed to travel to the Caribbean to meet David, but the trip never occurred. Victim 6 sent $1,500 via Walmart to EMENI, whom she did not know.

(b) On April 14, 2018, Victim 6 sent $5,100 to Kenneth EMENI at an address in Huntington, WV through MoneyGram; She sent this money to Kenneth EMENI at the direction of David, who told Victim 6 that Emeni would forward the money to him.

(c) On April 24, 2018, David asked Victim 6 for $1,500.00 to pay for travel roundtrip travel to the Caribbean. Victim 6 sent $1,500 via Western Union to EMENI.

(d) On April 26, 2018, David asked Victim 6 for $1,500.00 to pay for roundtrip travel to the Caribbean. Victim 6 stated she sent this $1,500 via Western Union to EMENI.

(e) On May 1, 2018, David asked Victim 6 to send $200 to his daughter in Texas because she needed cash for school. Victim 6 stated she sent his money to David's daughter's teacher, Dawn Marie Perdue.

(f) On June 7, 2018, David asked Victim 6 to send $1,348 to him because the United Kingdom Bank was shutting down and his funds had to be withdrawn immediately. David told Victim 6 he had to pay half of this fee to retrieve his life savings, which he had in this bank. Victim 6 is unsure where she sent this money to but she did not send the money directly to David. Victim 6 is also unsure if she sent a money order or currency.

(g) On June 11, 2018, Victim 6 purchased three $100 iTunes cards, which she sent to David. She believes she sent these iTunes cards to a Huntington, WV address.

(h) On June 12, 2018, David asked Victim 6 to send $1,374.96 to him because the United Kingdom Bank was shutting down and his funds had to be withdrawn immediately. David told Victim 6 he had to pay the remaining half of the fee to retrieve his life savings, which he had in this bank. Victim 6 is unsure where she sent this money to but she did not send the money directly to David. Victim 6 is also unsure if she sent a money order or currency.

(i) On June 29, 2018, she wired $20,000 to John NASSY Swift. The funds were deposited in NASSY's Chase Bank account number ending in 5723 held in Huntington, WV. David told Victim 6 that NASSY would forward him the money. Per David, the purpose of the wire transfer was "emergency funds needed to pay for lawyer and legal expenses to retrieve his funds out of the United Kingdom bank." This $20,000 was allegedly half of David's legal fees.

(j) On July 3, 2018, she wired $20,000 to NASSY's Chase Bank account number ending in 5723 held in Huntington, WV. David told Victim 6 this $20,000 wire transfer was to pay the remaining legal fees for removing his money from the United Kingdom Bank.

(k) On July 10, 2018, she wired $5,000 to NASSY's Chase Bank account number ending in 5723 held in Huntington, WV.

(l) On August 3, 2018, she sent a wire transfer for $10,000 to John NASSY Swift. These funds were deposited in NASSY's Chase Bank account number ending in 5723 held in Huntington, WV. David told Victim 6 the purpose of this wire transfer was to pay for a transporter to bring the funds to the United States from the United Kingdom Bank.

(m) On September 6, 2018, Victim 6 sent a wire transfer for $30,000 to Oluwabamishe AWOLESI's Chase Bank account ending in number 2389, held in Huntington, WV. Victim 6 stated that David told her to send this wire transfer to NASSY or EMENI and she attempted to do so. When the wire transfer would not go through to

NASSY or EMENI, she contacted David about the problem. David then instructed her to send this wire transfer to AWOLESI even though she did not know him. David told her AWOLESI would forward the money to him. David told Victim 6 the purpose of this wire transfer was to pay additional Customs fees pertaining to the funds transfer from the United Kingdom to the United States.

(n) On September 10, 2018, Victim 6 wired $30,000 to AWOLESI's Chase Bank account ending in number 2389 held in Huntington, WV. Victim 6 stated that David told her to send this wire transfer to NASSY or EMENI and she attempted to do so. When the wire transfer would not go through to NASSY or EMENI - she contacted David about the problem. David then instructed her to send the wire transfer to AWOLESI even though she did not know him. David told her that AWOLESI would forward the money to him. David told Victim 6 the purpose of this wire transfer was to pay additional Customs fees pertaining to the funds transfer from the United Kingdom to the United States.

(o) On September 17, 2018, she wired $30,000 to AWOLESI's Chase Bank account ending in number 2389 held in Huntington, WV. Victim 6 stated that David told her to send this wire transfer to NASSY or EMENI and she attempted to do so. When the wire transfer would not go through to NASSY or EMENI, she contacted David about the problem. David then instructed her to send the wire transfer to AWOLESI even though she did not know him. David told her that AWOLESI would forward the money to him. David told Victim 6 the purpose of this wire transfer was to pay additional Customs fees pertaining to the funds transfer from the United Kingdom to the United States.

(p) On November 12, 2018, she sent a Fed Ex package to a John Akrah at 1510 7th Ave Apt 6 in Huntington, WV 25701. The cost of this package was $40.85 and she cannot recall what was inside the package. Victim 6 does not know who John Akrah is, as it was a name given to her by David when he instructed her to send the package.

(q) On November 23, 2018, she sent a package via US Postal Express mail costing $24.70 to a John Akrah at 1510 7th Avenue Apt 6 in Huntington, WV 25701. Victim 6 sent this package at David's direction. She has never met John Akrah and she does not know who he is.

33. Victim 6 stated she sent David currency but she cannot recall the amount of currency sent or where she sent the currency.

Victim 7

34. Victim 7 met a man on Instagram who she knew as Mason George ("Mason") around December 2018. Victim 7 communicated daily with Mason via text messages and on Apps such as What's Up. Mason told Victim 7 he worked on an Exxon Mobile oilrig in the Gulf of Mexico. Around December 2018, Mason told her his oilrig crew was running out of food and Victim 7 sent a wire transfer at Mason's request.

35. Victim 7 sent a wire transfer on August 28, 2019 for $9,000 to Kenneth OGUDU at Chase Bank in Huntington, WV. This document reflects the purpose of the wire transfer was "personal loan." Victim 7 told investigators that Mason told her to tell her bank that was the purpose of the wire transfer. Victim 7 stated that Mason called her on this date and advised he was on his way to Louisiana to see her when he was kidnapped by drug dealers in New Orleans. Mason told Victim 7 that the drug dealers gave him the phone so he could call her and get the ransom money. Mason asked Victim 7 to wire $9,000 to Kenneth OGUDU for his ransom. Victim 7 stated this purpose of the wire transfer on the form was false but she did as Mason requested. Victim 7 has never met or communicated with OGUDU.

36. Victim 7 wired $3,000 to OGUDU's Chase Bank account held in Huntington, WV on August 30, 2019. Victim 7 also wired another $10,000 to OGUDU on September 9, 2019. These wire transfer documents reflects the purpose of the wire transfers was "personal loan." Victim 7 stated that Mason called her again and advised her the kidnappers wanted more money. Mason told her to wire another $3,000.00 to OGUDU for the ransom. Victim 7 admitted the stated purpose of the wire transfer on the bank form was false but she did as Mason requested.

37. Victim 7 sent a wire transfer on September 9, 2019, for $10,000 to EMENI at City National Bank in West Virginia from her account at Mid-South Bank. This document reflects the purpose of the wire transfer was for a "personal loan." Victim 7 stated that Mason called her again on this date and advised her the kidnappers wanted even more money. Mason told her to send another $10,000 to EMENI to pay the ransom. Victim 7 stated this purpose of the wire transfer on the bank form was false but that Mason told her to tell her bank that was the purpose of the wire transfer. Victim 7 stated this purpose was false but she did as Mason told her to do. Victim 7 has never met or communicated with Kenneth EMENI.

38. Victim 7 stated that Mason called her and advised he had been kidnapped by drug dealers again on his way to see her in Louisiana. Mason told her a man named Benjamin was going to come to her house to get the ransom money. When Benjamin never showed up Mason called Victim 7 again and asked Victim 7 to wire $12,000 for the ransom to AMECHI. On February 21, 2020, Victim 7 wired AMECHI $12,000 even though she never met or communicated with him.

Victim 8

39. Victim 8 owned and operated a nail salon in the Houston, TX area for many years. In November 2019, Victim 8 met Barry Nguyen ("Nguyen") on Instagram and Facebook. Nguyen told Victim 8 he was an engineer from California and he was involved in mining diamonds. Nguyen introduced her to Teresa Janelle Carpenter ("Teresa") from Wisconsin. Teresa told Victim 8 she moved to Florida to work for a Bit Coin company. After Nguyen made the introduction to Teresa, Teresa communicated with Victim 8 extensively to get Victim 8 to invest her own money

in Bit Coin. Teresa texted Victim 8 information that if she invested $10,000 in Bit Coin in seven days her investment would make $50,000. Teresa sent Victim 8 copies of what Teresa claimed were her Wisconsin Driver's License, and Florida Trading License.

40. Victim 8 sent 13 wire transfers to EMENI, who resided in Huntington, WV, at Teresa's direction, even though she had never met him or communicated with him. These wire transfers totaled $290,300 which are detailed in the table below. Victim 8 stated that each of these wire transfers were sent to purchase Bitcoin. Teresa texted Victim 8 before each transfer, and instructed her to tell the bank officials that the purpose of the wire transfers was to make purchases. Teresa also regularly texted Victim 8 regarding the profits she made from her Bitcoin investments, but Victim 8 never received any return or profits from these "investments."

Date	Amount	Recipient	Stated Purpose
1/9/2020	$10,000	EMENI	Purchase
1/11/2020	$10,000	EMENI	Purchase
1/13/2020	$10,000	EMENI – sent from Victim 8's business account	Purchase
1/21/2020	$10,400	EMENI	No purpose stated
1/22/2020	$10,000	EMENI	Purchasing Personals
1/27/2020	$10,000	EMENI	Purchase
1/29/2020	$9,000	EMENI	Purchase
2/3/2020	$19,400	EMENI	None stated
2/7/2020	$28,000	EMENI – sent from Victim 8's business account	Purchase
2/13/2020	$35,000	EMENI	None stated

2/18/2020	$40,000	EMENI	Purchase
3/3/2020	$50,000	EMENI	Purchasing Merchandise
3/12/2020	$48,500	EMENI	Purchasing
TOTAL	**$290,300**		

Victim 9

41. Victim 9 met someone who went by the name "Teddy Drey" ("Drey") online around September 2019. After communicating several times, Drey asked Victim 9 if he wanted to invest some money in bitcoin and Drey promised Victim 9 that he could double his money in 2-4 weeks. The email address used by Drey was teddydrey90@gmail.com. Victim 9 stated he sent $1,000 via a wire transfer from his bank account in Michigan to Augustine AMECHI in Huntington, WV at Drey's direction, even though he did not know AMECHI. Drey told Victim 9 that AMECHI would get the $1,000 investment to Drey.

42. Before sending the wire transfer, Victim 9 texted Drey that he was concerned about sending the wire transfer because they had just met online and he was concerned the funds would end up in somebody's bank account. Drey responded "you are in safe hands my friend." Drey suggested that Victim 9 could contact three people via email who were his previous clients. Those email address were: johncolns286@gmail.com; ginar4940@gmail.com and jj1082427@gmail.com. Victim 9 did not reach out to these individuals.

43. Drey previously instructed Victim 9 to send the wire transfer to a Michelle Bump's account in North Dakota. When Victim 9 had trouble completing the wire transfer at his credit union Drey texted Victim 9 and told him to wire AMECHI the funds in Huntington, WV.

Victim 10

44. In the fall of 2019, Victim 10 met a man online, who went by the name Ryan Simon. She stated they communicated through a social media site several times a week. On about October 30, 2019, Mr. Simon asked her to send him some money via a wire transfer and he told her to send the money to a Kenneth EMENI at City National Bank in West Virginia. Victim 10 did not know EMENI nor had ever communicated with him. On October 30, 2019, Victim 10 wired EMENI $4,000.00 from her bank in Maryland.

Victim 11

45. Victim 11 started communicating with a man who introduced himself as James Morrison, ("Morrison") online in early 2019. Morrison contacted her several times a week initially, and then communicated with her sometimes several times a day and a romance developed. The romance ended in July 2020. Morrison told Victim 11 he owned a construction company in Ohio, but that he was taking a construction job in Turkey. He told Victim 11 that he could not use his credit card in Turkey and thus, could not pay his hotel bills and living expenses.

46. Victim 11 stated she sent money at Morrison's direction on several occasions. She never sent any money directly to Morrison. Victim 11 believes she sent three or four wire transfers to others at Morrison's direction. On July 9, 2019, Victim 11 sent a $50,000 Cashier's check, made payable to Kenneth OGUDU that she purchased from her bank, the Louisiana Federal Credit Union at Morrison's direction. Morrison told Victim 11 to put OGUDU as the payee and she mailed this check to OGUDU in Huntington, WV. She does not know or ever met OGUDU. Morrison told Victim 11 that OGUDU would then get these funds to Morrison, and bank records

reveal that OGUDU deposited this $50,000 Cashier's check into his bank account and did not make a subsequent $50,000 transfer to any individual.

Victim 12

47. Victim 12 sent the following wire transfers from her bank in Pennsylvania to EMENI , HARRISON, NASSY and OGUDU in Huntington, West Virginia:

Date	Amount	Recipient	Stated Purpose
April 15, 2019	$6,400	EMENI	Purchase of Equipment
April 18, 2019	$4,700	HARRISON	Purchase of Equipment
May 1, 2019	$8,400	EMENI	Purchase of Equipment
May 9, 2019	$5,000	EMENI	Purchase of Equipment
May 13, 2019	$4,000	EMENI	Purchase of Equipment
May 20, 2019	$4,500	EMENI	Purchase of Equipment
May 28, 2019	$7,000	NASSY	Purchase of Equipment
August 28, 2019	$3,000	OGUDU	Purchase of Equipment
November 12, 2019	$6,000	OGUDU	Purchase of Equipment
December 19, 2019	$5,000	EMENI	Purchase of Equipment
December 20, 2019	$4,100	EMENI	Purchase of Equipment

48. During Victim 12's interview, she stated that she was not a victim of fraud but sent these wires to order equipment for her restaurant. However, Victim 12 could not remember what pieces of equipment she ordered with the wire transfers. Thus, Victim 12 is classified as a victim for the purposes of this affidavit, but the investigation may later reveal that she is a co-conspirator.

Victim 13

49. Victim 13, who resides in Michigan, told investigators that she met a man, who identified himself as Daniel Moore ("Moore"), online in 2016. Moore told Victim 13 he was a civil engineer and he was working on an oilrig in Dubai. Victim 13 and Moore talked frequently over the phone, email and text messaging. Moore told Victim 13 he was from Grand Rapids, MI and he would be coming back home soon. About one month after meeting Moore, Moore started asking for money to pay his workers. Victim 13 sent money at Moore's direction via Money Gram and wire transfers. She never sent the money directly to Moore, it was always sent to other people at Moore's direction. Moore assured Victim 13 that the recipients would forward the funds to him.

50. Victim 13 stated that Moore allegedly died in December 2017. Shortly after learning of Moore's death, Victim 13 was contacted by a female named "Ieasha," who also claimed to be from Dubai. Ieasha advised Victim 13 that Moore's employer owed Moore a large amount of money (about $3,000,000) and that Moore listed Victim 13 as his beneficiary. Ieasha told Victim 13 she (Ieasha) would help Victim 13 collect the money from Moore's estate. Before Victim 13 could get these funds, she had to pay the Dubai government taxes of around $5,000.

51. Victim 13 stated she sent the following amounts of money at Ieasha's direction. Victim 13 never sent the funds directly to Ieasha, instead Ieasha instructed Victim 13 to send the money to the individuals listed below and then claimed these individuals would forward the money her. Victim 13 never met EMENI, HARRISON or Romello Thorpe (Thorpe) but transferred funds to these individuals pursuant to Ieasha and Moore's instructions.

Date	Recipient	Amount	Method	Purpose
8/19/17	EMENI	$900	Western Union	Pay Moore's workers
12/14/17	HARRISON	$725	Money Gram	Pay Moore's workers
1/18/18	EMENI	$34,500	Wire transfer	Taxes for $3,000,000 she inherited from Moore per Ieasha
9/13/19	Thorpe	$35,000	Wire Transfer	Ieasha instructed Victim 13 to tell the bank that the purpose of the transfer was for a Quilting machine and Victim 13 cannot recall the true purpose of the transfer

52. After Victim 13 wired Romello Thorpe $35,000 on September 13, 2019, Thorpe made three electronic payments to Kenneth OGUDU with these fraud proceeds. On September 19, 2019, he sent two separate payments to OGUDU, one for $2,000 and one for $5,000. On September 20, 2019, he made another payment of $7,000 to OGUDU.

Victim 14

53. Victim 14 started communicating with a man online in 2015, who told her that his name was Blake Shelton ("Shelton"), the country music star. Shelton told Victim 14 he was going to send her a VIP pass for one of his concerts. Victim 14 eventually was virtually introduced to Heather Harrison ("Heather"), who allegedly worked for Warner Brother's music.

54. In the summer of 2018, Heather told Victim 14 that she was going to be entered in the contest to win the Blake Shelton Fan of the Year if she paid a fee of $2,500. In September 2018, Heather told her that if she wired $2,500 she would become a member of the Blake Shelton Fan Club and be entered into the Blake Shelton Fan Club $1,000,000 contest. Heather told Victim 14 to send the wire transfer to Oluwangabenga HARRISON. Heather then provided Victim 14

with HARRISON's receiving bank routing number and the account information for a bank in West Virginia. On September 12, 2018, Victim 14 wired HARRISON $2,500 from her Alabama bank.

55. Victim 14 believes in late September 2018, Heather told Victim 14 if she sent another $5,000 wire transfer, she would be in the top 10 of the $1,000,000 Blake Shelton Fan Club Fan of the Year contest. Heather again directed Victim 14 to wire $5,000 to HARRISON's West Virginia bank account. On October 9, 2018, Victim 14 wired HARRISON the $5,000.

56. Around October of 2018, Heather told Victim 14 if she sent a $10,000 wire transfer, she was going to be in the top three of the $1,000,000 Blake Shelton Fan Club Fan of the Year contest. Heather again instructed Victim 14 transfer the $10,000 to Oluwangabenga HARRISON. Victim 14 transferred $10,000 to HARRISON on October 23, 2018.

57. In early 2020, Heather contacted Victim 14 again and told her that she had won $250,000 in the Blake Shelton Fan of The Year contest. Heather informed Victim 14 she needed to wire $12,000 to pay the taxes on her winnings. Victim 14 refused to send any more funds.

Victim 15

58. In early November 2019, Victim 15 went online to look for an apartment to rent in Bellingham, WA because she was in the process of moving to the State of Washington. A man responded to her contact for the apartment. They communicated through email and the person emailed her a contract for the lease of the apartment. On November 19, 2019, she sent a wire transfer for $2,300 to Kenneth EMENI. After Victim 15 wire transferred the funds she had no further contact from EMENI. Victim 15 checked out the address for the property she was trying to rent and the apartment belonged to a couple who were not familiar with EMENI.

Victim 16

59. Victim 16, who resides in the State of Washington, stated that she first met someone, who identified himself as John Weisner ("Weisner"), online in June 2018. Weisner told Victim 16 he was from Florida originally and he was a petro chemical engineer. Weisner told Victim 16 he was going back to Manitoba Canada to work on an oilrig and he was coming to the State of Washington to see her and marry her before he returned to Canada. Victim 16 stated she and Weisner communicated via text messages, emails and spoke on the phone most every day and sometimes multiple times a day. Weisner repeatedly asked Victim 16 to send him money to pay his workers but Weisner always asked Victim 16 to send the money to other people, instead of directly to Weisner.

Date	Recipient	Amount	How Funds Were Transmitted	Purpose
9/2/18	NASSY	$2,500	Wal-Mart Money Gram	Pay Weisner's oilrig workers
9/3/18	NASSY	$2,500	Wal-Mart Money Gram	Pay Weisner's oilrig workers
9/12/18	NASSY	$2,500	Mailed Cashier's check to NASSY in Huntington, WV	Pay Weisner's oilrig workers
9/14/18	NASSY	$2,500	Mailed Cashier's check to NASSY in Huntington, WV	Pay Weisner's oilrig workers

Victim 17

60. Victim 17 stated she met a man online, but that she could not remember his name. She advised he began flirting with her and asked her to communicate via WhatsApp and through Google Hangouts. She further advised they communicated for approximately two months. Victim 17 stated he asked her for money to pay for his travel back to the United States and for a new

phone for his son because his son's phone quit working. She further stated he provided her with the wire instructions and she wired the money as he instructed. She confirmed the wire was sent from her PNC Bank for $7,500. She did not specifically recall whom she sent the wire to but indicated the name Kenneth EMENI sounded familiar when asked.

Victim 18

61. In December 2019, Victim 18 met a man online who went by the name of Carlos Davis ("Carlos"). Carlos told Victim 18 that he has been working as a neurosurgeon for the United Nations in Iraq for 2 years. Victim 18 communicated daily with Carlos through text messages. Sometimes Carlos emailed her as well using the email carloscdavis0@gmail.com and forwarded her his "barrister's" email, Barister-Terry@outlook.com. About a month into their virtual courtship, Carlos told Victim 18 he needed money for his living and traveling expenses in Iraq, as well as for fees for him to leave Iraq so he could return to the United States. Carlos asked her to send him $7,500 via a wire transfer to his friend, Kenneth EMENI. Carlos told Victim 18 that EMENI would give him the $7,500 because Carlos did not have access to his U.S. based bank accounts in Iraq. Carlos provided Victim 18 with EMENI 's financial information, including his bank, the bank's routing number and his account number. On January 15, 2020, Victim 18 wired $7,500.00 to EMENI 's bank account in Huntington, WV from her bank in California.

62. Victim 18 stated that in February 2020, Carlos asked her to send two more wire transfers for $6,000.00 each (for $12,000 total) because he needed money to pay an Iraq exit fee and for a marriage certificate. She sent these two $6,000 wire transfers from her Chase Bank

account as Carlos directed, but she cannot recall whom she sent the wire transfers to or which bank.

Victim 19

63. Victim 19 was contacted via email early in 2020 by a representative of Link Cargo Express, a Texas company. She advised that the company representative asked her to send some money but she could not recall for what purpose. Victim 19 solely communicated with the company representative through email. The representative of Link Cargo instructed Victim 19 to send two wire transfers to Augustine AMECHI, even though she had never met AMECHI. Victim 19 wired $1,500 to AMECHI's City National account ending in 5827 on April 23, 2020 from her Texas bank. Victim 19 then wired an additional $4,750 to AMECHI on April 28, 2020.

Victim 20

64. Victim 20, who resides in Illinois, stated that she first met became with romantically involved with someone she knew as Maurice Idress ("Maurice") a couple of years ago online. Maurice told Victim 20 he was working in New York. Maurice and Victim 20 communicated almost every day via her cell phone. Shortly after she started communicating with Maurice, he asked her for money so he could pay his employees. Maurice always told her to send the money to EMENI , who would then send the funds to him. Victim 20 made the following financial transactions to EMENI at Maurice's direction:

Date	Recipient	Amount	How Funds Were Transmitted
11/3/17	EMENI	$750	Walmart
11/4/17	EMENI	$750	Money Gram

11/8/17	EMENI	$500	Mailed Cashier's check to NASSY in Huntington, WV
11/9/17	EMENI	$500	Mailed Cashier's check to NASSY in Huntington, WV
5/1/18	EMENI	$5,000	Wire from her bank in Kentucky to EMENI

Victim 21

65. Victim 21 started an online romance with a man, who introduced himself as Gregory Hulson ("Gregory") in mid-2017. Gregory told Victim 21 that he was originally from Canada and now working on an oilrig in the Gulf of Mexico as a safety inspector. Gregory and Victim 21 communicated daily through Google Hangouts, telephone and text messages.

66. Victim 21 stated that after she and Gregory had been communicating for about 6 months, Gregory asked her for money so he could purchase supplies since he was on an oilrig and he could not access his bank accounts. Gregory asked her to wire $12,000 to Oluwangbenga HARRISON and HARRISON would get the $12,000 to Gregory. Gregory then provided her the bank routing information and account number for HARRISON's West Virginia bank accounts. On July 17, 2018, Victim 21 wired HARRISON $12,000 from her bank account held in Tennessee.

Victim 22

67. Victim 22 met someone who introduced himself as Harry Cong Chu ("Harry") online. They talked for about six months through Facebook, Google Hangouts and text messages. According to Victim 22, Harry lived in New York but then claimed to have moved overseas. Harry told Victim 22 he needed money to come back to the United States. Harry borrowed approximately $30,000 to $40,000 from Victim 22, and never paid Victim 22 back.

68. After initially denying the transfers, Victim 22 later admitted that she sent money to Harry through Western Union money transfers approximately two or three times. Victim 22 informed investigators that she sent Kayode AKANBI money a few times. Harry claimed he needed money but did not have an account and instructed Victim 22 to send money to Harry's "agent" who would help Harry get back to the United States. Victim 22 said she wrote checks to AKANBI at least twice, for Harry. One payment was via a personal check dated in April 2019 for $5,000 and the second payment was in May 2019 for $7,000, which was also made via personal check. Harry also asked Victim 22 to wire funds to AMECHI and OGUDU's Chase Bank accounts held in Huntington, West Virginia.

69. Victim 22 also informed investigators that she received $10,000 twice and deposited those funds into her Chase Bank account. Harry had asked for her bank account information and then asked her if she had received some money. After Victim 22 confirmed she received the money, Harry told her to transfer the money to another bank account in Africa. Victim 22 eventually traveled to the New York address Harry had given her, and knocked on the door. However, the people who lived there said they didn't know him.

Victim 23

70. Victim 23 lives in Florida. Financial records revealed that OGUDU received a substantial amount of funds from Victim 23. For example, Victim 23's Zelle account sent 34 transactions to Kenneth OGUDU, which totaled to $43,531.00. Victim 23 told investigators that she was unaware of the Zelle transfers but that she gave her boyfriend, Martin Nguyen her financial information and told him how to access her accounts. Victim 23 also told agents that she no longer

knows how to access her bank accounts. Victim 23's Chase Bank account also sent three wires to Kenneth OGUDU's personal bank account at Fifth Third Bank. On August 26, 2019, Victim 23 sent $9,100 to OGUDU, followed by another transfer of $6,300 to OGUDU on September 3, 2019, and a final transfer of $14,000 to OGUDU on September 10, 2019.

71. A substantial amount of the funds OGUDU received from Victim 23 stemmed from incoming deposits into Victim 23's Chase Bank account ending in number 7389. These deposits into Victim 23's Chase Bank account originated from victims located throughout the United States and abroad. Thus, in my training and experience Victim 23 appears to be acting as a money mule[2] for OGUDU and others.

72. For example, Victim 13 wired $31,000 to Victim 23 on September 3, 2019. Afterwards, several payments were made to OGUDU from Victim 23, including a wire transfer to Ogudu on September 3, 2019 for $6,300; a $14,000 wire transfer to Ogudu on September 10, 2019, and several other transfers to OGUDU from Zelle and other mobile payment processing websites. It should also be noted that there is another victim besides Victim 13 who also sent money directly to OGUDU and Victim 23's Chase Bank account. After these funds reached Victim 23's Chase Bank account, they were subsequently transferred to make payments to OGUDU.

Victim 24

73. Victim 24 died in 2019. Her sister advised investigators that Victim 24 met a man online who claimed to be Benjamin Randolph Mixon of Atlanta, GA. Victim 24's sister knew this

---

[2] At this point in the investigation, it is unclear whether Victim 23 was acting as a willing or unwilling money mule for OGUDU and others.

information and the information below because she was in charge of overseeing Victim 24's financial affairs. Victim 24's sister also provided a copy of a document allegedly from the International Commercial Bank in Ghana, which represents that Victim 24 will receive $1,200,000. This document connected to two emails Victim 24 received wherein she was asked to send $3,850 to obtain the inheritance certificate and collect the funds.

74. Victim 24's sister also provided a copy of a letter from the International Monetary Fund wherein Victim 24 was advised she will not receive the $1,200,000 because she did not pay the required $47,000 to obtain the Anti-Terrorism and the Money Laundering Certificate. Victim 24 sent a Walmart money transfer for $1,000.000 to EMENI on June 19, 2017. Victim 24 also sent $1,000 via Money Gram to EMENI on June 17, 2019.

Victim 25

75. Victim 25, who resides in New Zealand, met a man online she knew as Mark Williams ("Mark") around June or July 2018 who she communicated with through Facebook and WhatsAp. Mark also communicated with her through the email address, markwilliams3672@gmail.com. Williams informed her that he made money through Bitcoin trading and put her in contact with a woman that Victim 25 knew as Inayee Smith, who could help her make a profit from Bitcoin investments as well. Victim 25 informed law enforcement that she purchased around $96,000 in Bitcoin around November or December of 2018. Inayee communicated with Victim 25 through the email addresses of binaryautotrader65@gmail.com, smithinayee@gmail.com and jackwils1598@gmail.com. Mark helped Victim 25 set up a Bitcoin wallet afterwards and then Inayee sent her an email around December 19, 2018, instructing her to

obtain the Bitcoin through localbitcoins.com. Victim 25 then purchased the Bitcoin, put them in her Bitcoin wallet and then transferred them to Inayee's Bitcoin wallet. Victim 25 never received any funds back from her investment.

76. Someone Victim 25 knew as Colin Bradson ("Colin") contacted her online around January 1, 2019. Victim 25 confided in Colin about the bitcoin investment and he told her that she had been scammed but that he knew people who could help her get her money back. Colin then instructed her to send funds to NASSY, HARRISON, EMENI and an individual named Frednie Rene. Colin provided Victim 25 with the bank routing number, bank accounts, names on the accounts, addresses on the account, the amounts to send and the receiving bank SWIFT codes. Cumulatively, Victim 25 wired $161,500 to NASSY, HARRISON, EMENI and $3,000 Frednie Rene in this "fraud recovery" scam. Victim 25 sent all of the wires to NASSY, HARRISON and EMENI 's bank accounts held in Huntington, WV.

FINANCIAL ANALYSIS

77. At least from 2017 to the summer of 2020, NASSY, OSUMANU , AKANBI, AMECHI, HARRISON, EMENI , OGUDU, AFOLABI and AWOLESI operated fraud scheme(s) and the information below summarizes the amount of proceeds each subject received from illegal activity. Investigators' review of EMENI, NASSY, HARRISON, AMECHI, AKANBI, AFOLABI, OSUMANU and OGUDU reported wages for the period from 2017 through March 21, 2020 revealed low wages for all of these individuals.

John NASSY

78. A review of NASSY's known bank accounts shows that he received wires or other deposits from at least 16 different individuals currently believed to be fraud victims from June 29, 2018 until May 29, 2019, which total to approximately $167,746.30 at this time. However, as the financial breakdown below shows, NASSY is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. Pursuant to a check through the U.S. Department of Labor, NASSY had wages totaling $10,099.88 during the period 2017 through March 31, 2020.

Deposits Received from Victims		$167,746.30
Cash Deposits		$129,508.00
Deposits from Co-Conspirators		$ 45,709.99
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$286,641.79	
Total Illegal Proceeds Received by NASSY		**$629,606.08**

Abdul OSUMANU

79. A review of OSUMANU's known bank accounts shows that he received wires or other deposits from at least two different individuals currently believed to be fraud victims from September 5, 2018 until May 30, 2019, which total to approximately $30,112 at this time. However, as the breakdown below shows, OSUMANU is believed to have received more fraud proceeds through other means such as cash deposits. Pursuant to a check through the U.S. Department of Labor, OSUMANU had wages totaling $0 during the period 2017 through March 31, 2020.

Deposits Received from Victims	$ 30,112.00

Cash Deposits	$ 4,180.00
Deposits from Co-Conspirators	$ 0.00
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$ 6,578.55
Total Illegal Proceeds Received by OSUMANU	**$ 40,870.55**

Kayode AKANBI

80. A review of AKANBI's known bank accounts shows that he received wires or other deposits from at least five different individuals currently believed to be fraud victims from April 19, 2019 until July 12, 2019, which total to approximately $27,544.78 at this time. However, as the financial breakdown below shows, AKANBI is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. Pursuant to a check through the U.S. Department of Labor, Kayode AKANBI had wages totaling $581.80 during the period 2017 through March 31, 2020.

Deposits Received from Victims	$ 27,544.78
Cash Deposits	$ 48,660.00
Deposits from Co-Conspirators	$ 28,258.35
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$110,769.76
Total Illegal Proceeds Received by AKANBI	**$215,232.89**

Augustine AMECHI

81. A review of AMECHI's known bank accounts shows that he received wires or other deposits from at least 37 different individuals currently believed to be fraud victims from February 19, 2019 until July 7, 2020, which total to approximately $108,601.92 at this time. However, as

the financial breakdown below shows, AMECHI is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. Pursuant to a check through the U.S. Department of Labor, Augustine AMECHI had wages totaling $5,166.87 during the period 2017 through March 31, 2020.

Deposits Received from Victims		$108,601.92
Cash Deposits		$105,718.03
Deposits from Co-Conspirators		$ 0.00
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$159,983.08	
Total Illegal Proceeds Received by AMECHI		**$374,303.03**

Oluwangabenga Harrison

82. A review of HARRISON's known bank accounts shows that he received wires or other deposits from at least 34 different individuals currently believed to be fraud victims from September 22, 2017 until June 11, 2019, which total to approximately $247,210.63 at this time. However, as the financial breakdown below shows, HARRISON is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. Pursuant to a check through the U.S. Department of Labor, HARRISON had wages totaling $45,380.35 during the period 2017 through March 31, 2020 and received wages of $27,138.63 during the first quarter of 2020.

Deposits Received from Victims	$247,210.63
Cash Deposits	$ 59,660.00
Deposits from Co-Conspirators	$ 45,925.43

Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$ 62,048.44
Total Illegal Proceeds Received by HARRISON	**$414,844.50**

Kenneth EMENI

83. A review of EMENI 's known bank accounts shows that he received wires or other deposits from at least 75 different individuals currently believed to be fraud victims from February 23, 2017 until March 12, 2020, which total to approximately $851,389.49 at this time. However, as the financial breakdown below shows, EMENI is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. Pursuant to a check through the U.S. Department of Labor, Kenneth EMENI has wages totaling $28,287.18 during the period 2017 through March 31, 2020.

Deposits Received from Victims	$851,389.49
Cash Deposits	$311,939.70
Deposits from Co-Conspirators	$ 42,050.07
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$398,242.19
Total Illegal Proceeds Received by EMENI	**$1,603,621.45**

Kenneth OGUDU

84. A review of OGUDU's known bank accounts shows that he received wires or other deposits from at least 12 different individuals currently believed to be fraud victims from May 30, 2019 until November 15, 2019, which total to approximately $253,448 at this time. However, as

the financial breakdown below shows, OGUDU is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle.

Deposits Received from Victims		$253,448.00
Cash Deposits		$ 5,308.00
Deposits from Co-Conspirators		$ 7,920.00
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$ 58,189.28	
Total Illegal Proceeds Received by OGUDU		**$ 324,865.28**

Abiodun AFOLABI

85. A review of AFOLABI's known bank accounts shows that he received wires or other deposits from at least 12 different individuals currently believed to be fraud victims from May 30, 2019 until November 15, 2019, which total to approximately $4,150 at this time. However, as the financial breakdown below shows, AFOLABI is believed to have received a much greater sum of fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. Pursuant to a check through the U.S. Department of Labor, Abiodun AFOLABI had wages totaling $2,712.35 during the period 2017 through March 31, 2020.

Deposits Received from Victims		$ 4,150.00
Cash Deposits		$ 19,638.00
Deposits from Co-Conspirators		$ 70,459.53
Deposits from Boss Revolution, Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$ 65,375.79	

Total Illegal Proceeds Received by AFOLABI **$ 159,623.32**

Oluwabanishe Taofik AWOLESI

86. A review of AWOLESI's known bank accounts shows that he received three deposits from one individual who is believed to be a fraud victim (Victim 6) for a total of $90,000 during the period of September 6, 2018 until September 17, 2018. However, investigators received information from a bank that AWOLESI was unemployed during this time. Moreover, AWOLESI appeared to structure several of his financial transactions after receiving these fraud proceeds.

Structured Transactions

87. Specifically, AWOLESI received three wire transfers of $30,000 each from Victim 6. These wire transfers occurred on September 6, 2018; September 10, 2018; and on September 17, 2018. As explained in the Victim Information Section, these funds came from Victim 6 wired to AWOLESI only after she was unable to send these wire transfers to NASSY or EMENI 's bank accounts in West Virginia as the scammer (David) instructed her.

88. After these wire transfers were deposited into AWOLESI's bank account at Chase Bank, AWOLESI conducted several cash withdrawals where he conducted the cash withdrawals in a manner where the bank did not file Currency Transaction Reports.

89. Through my training and experience, I know that banks have an obligation to report financial transactions over $10,000 by filing a CTR.

90. I also know through my training and experience that individuals will sometimes attempt to "structure" their financial transactions such as their withdrawals from bank accounts, and checks written to other individuals, to avoid the $10,000 reporting requirement. An example

of this can be seen when an individual makes two withdrawals of $5,000 close in time, instead of one withdrawal of $10,000.

91. In my training and experience, individuals will sometimes attempt to avoid the $10,000 because they do not wish to draw attention to their financial transactions.

92. Examples of the AWOLESI's structuring behavior are seen by the cash withdrawals listed below:

9/5/2018	$4,800.00
9/6/2018	$8,200.00
9/7/2018	$8,500.00
9/10/2018	$3,000.00
9/11/2018	$3,000.00
9/12/2018	$8,550.00
9/13/2018	$3,000.00
9/14/2018	$8,520.00
9/15/2018	$3,000.00
9/19/2018	$8,500.00
9/20/2019	$3,000.00
9/21/2018	$3,000.00
Total Cash Withdrawals	**$65,070.00**

BACKGROUND CONCERNING EMAIL

93. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts, like the email accounts listed in Attachment A.

94. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment

(including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

95. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

96. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a

result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

97. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant

insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE TO SEARCH TARGET EMAIL ADDRESSES

98. Based on the information obtained from witnesses and additional sources cited above, I have probable cause to believe that NASSY, OSUMANU , AKANBI, AMECHI, HARRISON, EMENI , OGUDU, AFOLABI and AWOLESI were involved in fraudulent and money laundering activities, in violation of 18 U.S.C. §§ 1341,1343, 1344, 1349, 1956 and 1957. I also have probable cause to believe that AWOLESI was involved in structuring in violation of 31 U.S.C. § 5324. I also have probable cause to search each of the Target Email addresses for the items described in Attachment B.

99. I believe from information I have learned from witnesses, other investigators, and financial records show that the fraudsters communicated with the fraud victims through the following email addresses, or referred the victims to contact these Victim Contact Email addresses, as explained in detail through the Victim Information Section. These facts, as well as others in the affidavit, provide probable cause to search these email addresses.

100. I believe from information I have learned from witnesses, other investigators, and financial records show that NASSY, OSUMANU, AKANBI, AMECHI, HARRISON, EMENI , OGUDU, AFOLABI and AWOLESI connected the Subjects Financial Contact Email Addresses to various bank accounts and mobile payment processing apps that they controlled. Through my

training and experience, as well as my review of financial records, I know that the financial institutions and mobile payment processing companies send bank statements and correspondence to customers and users' email addresses. These facts, as well as others in the affidavit, provide probable cause to search these email addresses.

CONCLUSION

101. Based on the forgoing, I request that the Court issue the proposed search warrant.

102. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

103. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to destroy or tamper with evidence, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

JEREMY THOMPSON
Task Force Officer
U.S. Secret Service

Subscribed and sworn to me telephonically on September 24, 2020

THE HONORABLE CHERYL EIFERT
UNITED STATES MAGISTRATE JUDGE